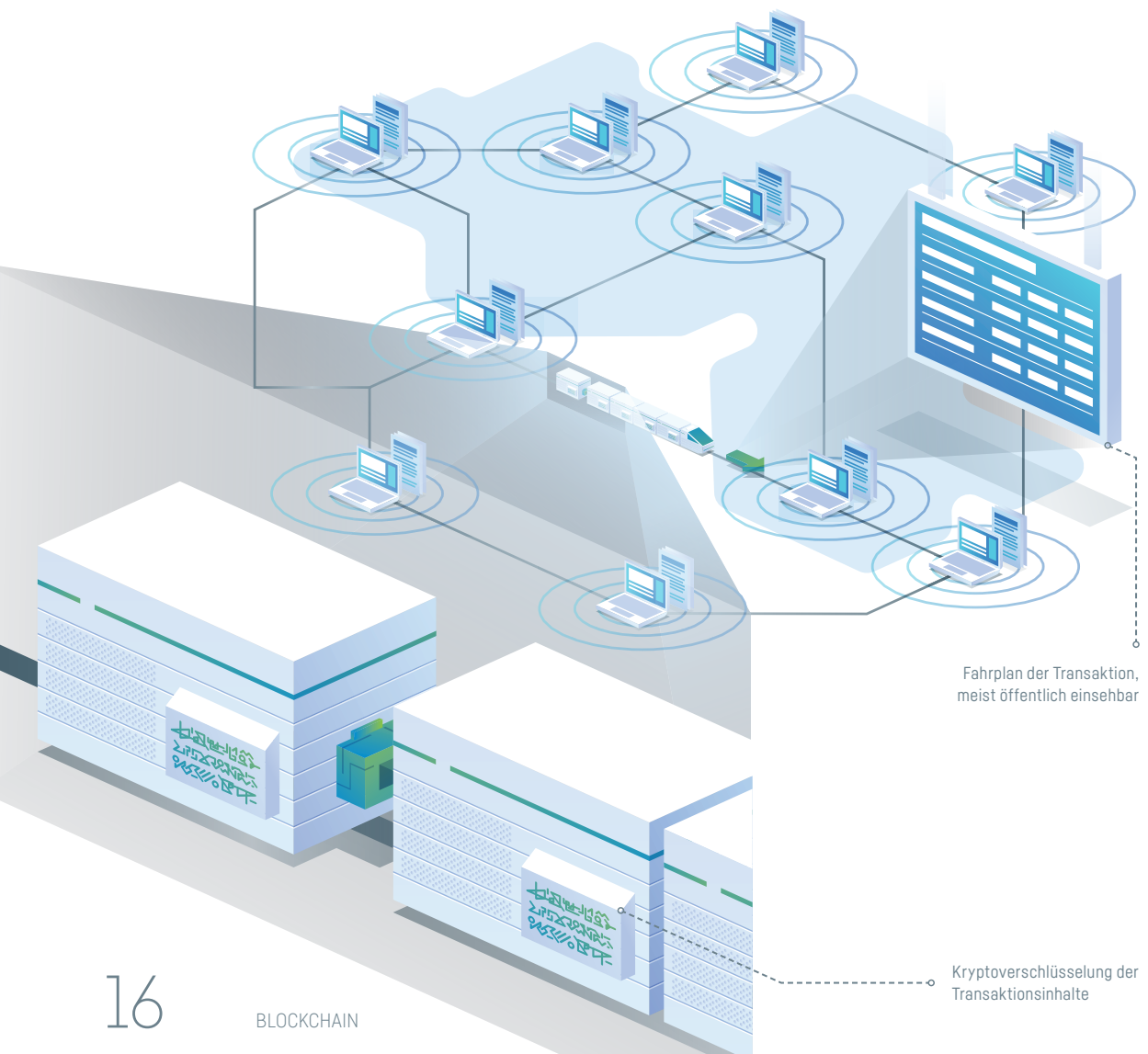


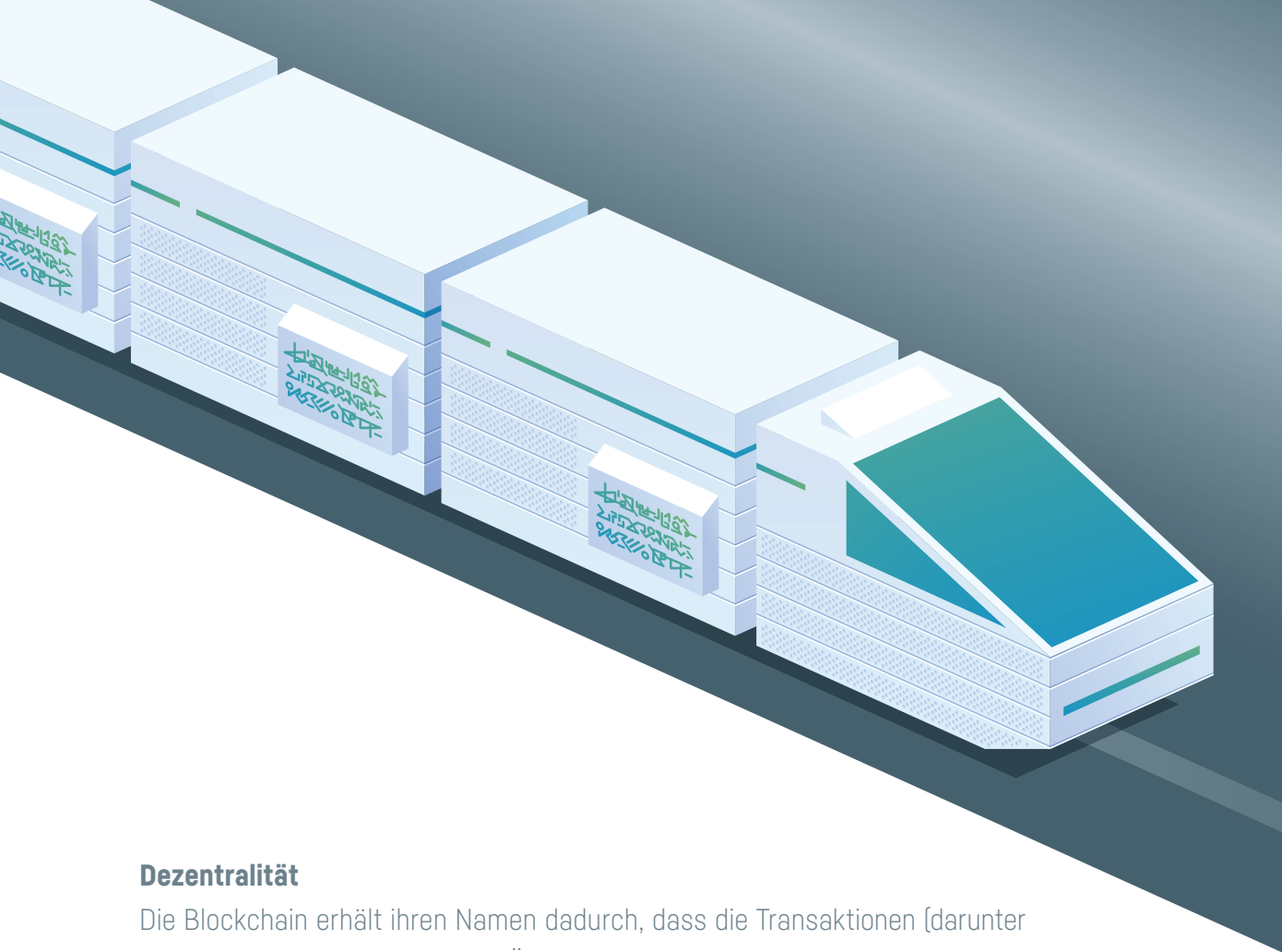
Blockchain – „like a Locked Train“

Text: Prof. Dr. Ali Sunyaev – Karlsruher Institut für Technologie (KIT)

Blockchain, Distributed Ledgers und kryptografische Verfahren

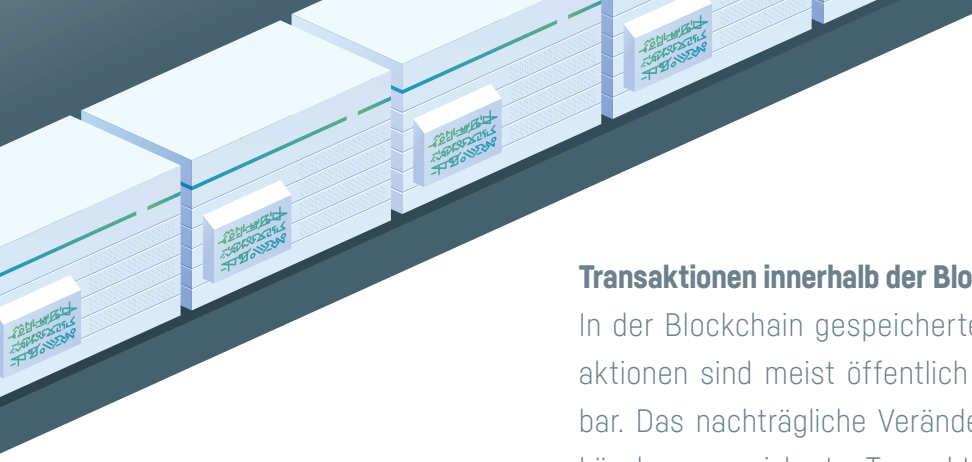
Blockchain ist ein Begriff, dem man in den vergangenen Jahren im Zusammenhang mit der Digitalisierung immer häufiger begegnete. Das Konzept wurde vor allem durch die Kryptowährung Bitcoin bekannt, die im Jahre 2008 vorgestellt und 2009 realisiert wurde. Doch was ist die Blockchain eigentlich und warum könnte sie bald einen großen Einfluss auf unseren Alltag haben?





Dezentralität

Die Blockchain erhält ihren Namen dadurch, dass die Transaktionen (darunter wird hier die Dokumentation der Übertragung von Daten verstanden, die dann mit Werten bzw. Assets assoziiert werden können) in Blöcken strukturiert abgelegt werden (engl. block) und eine Kette bilden (engl. chain). Es handelt sich dabei um ein Konzept der Datenhaltung, das in die „Distributed Ledger Technology“ (DLT) eingebettet ist. DLT ist die darunterliegende Technologie, die vor allem eine Lösung bereitstellt, um Konsens zwischen allen Knoten eines Distributed Ledgers zu schaffen, obwohl Knoten zeitweise nicht verfügbar sein können oder manche Knoten auch versuchen können, betrügerische bzw. falsche Daten einzubinden. Diese Fehler werden auch als „byzantinische Fehler“ bezeichnet. In der DLT wurden diese Probleme durch die Anwendung spieltheoretischer Konzepte (bspw. Byzantine Generals Problem) gelöst. DLT gilt daher als „Byzantine Fault Tolerant.“ Die Dezentralität verhindert Gefahren, die bei zentralisierten Infrastrukturen auftreten, zum Beispiel das, was im Technischen als „Single Point of Failure“ bezeichnet wird. Fällt ein zentrales System aus (engl. Point of Failure), auf das viele weitere Dienste zugreifen, die demnach stark abhängig davon sind, ist nicht nur das eigentliche System betroffen, sondern auch alle weiteren Dienste. Die Abhängigkeit von einer zentralen Instanz entfällt bei der DLT.

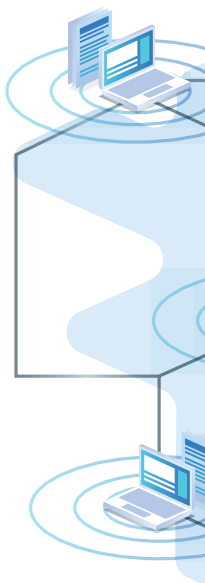


Transaktionen innerhalb der Blockchain

In der Blockchain gespeicherte Transaktionen sind meist öffentlich einsehbar. Das nachträgliche Verändern oder Löschen gespeicherter Transaktionen ist durch die Anwendung kryptografischer Verfahren jedoch nahezu unmöglich. Eine einzelne Transaktion enthält bei der DLT immer die Adressen von Sender und Empfänger, aber auch weitere Daten, die unverfälscht mittransferiert und bereitgestellt werden sollen. Üblicherweise hat jede Transaktion mindestens einen Vorgänger und kann mehrere Nachfolger haben, die immer mit den Daten des Vorgängers in Zusammenhang stehen müssen. Über diese Verkettung kann unveränderlich nachvollzogen werden, wohin welche Daten transferiert wurden.

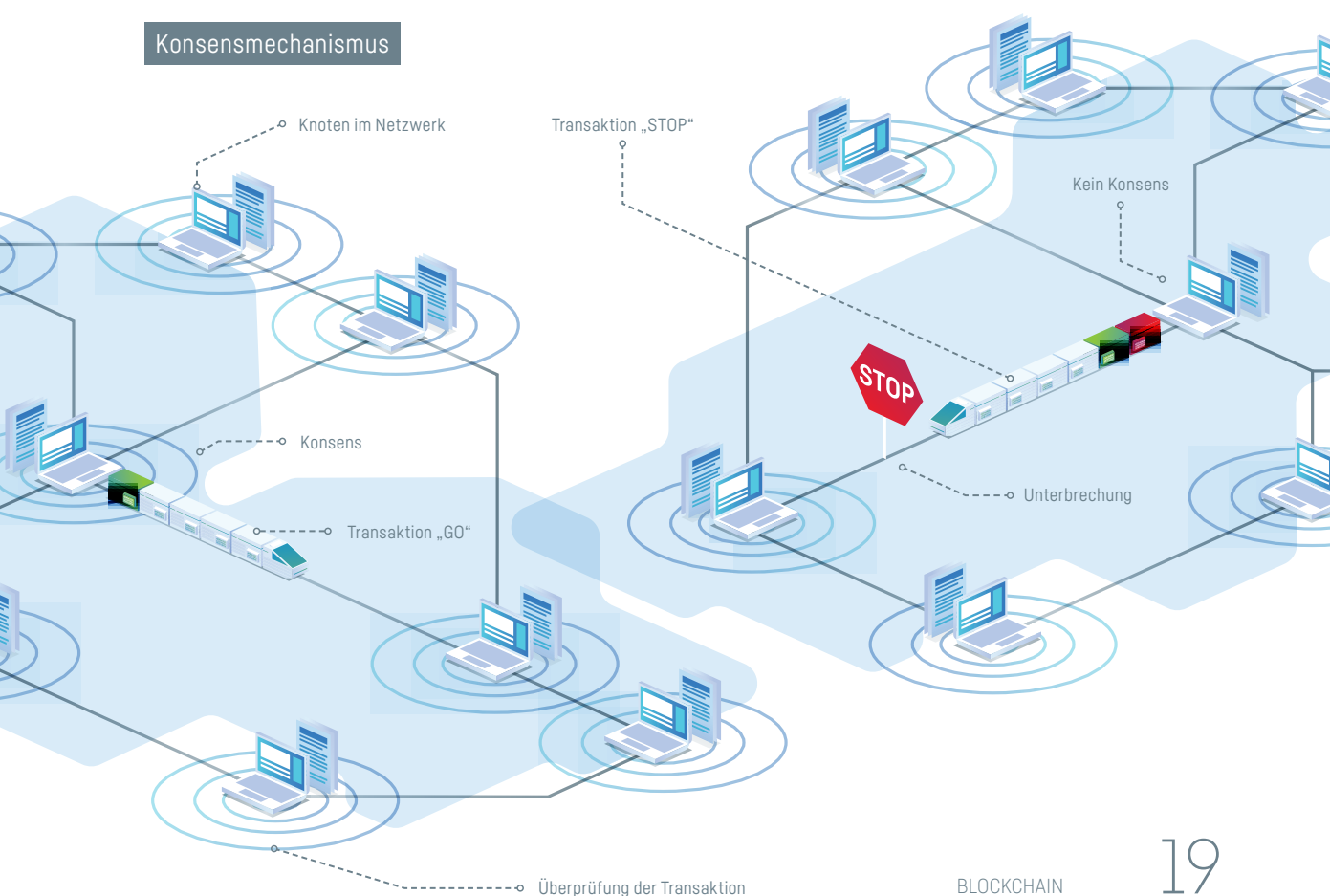
Transparenz

Derzeit erfordern viele Prozesse die Anwesenheit einer dritten, unabhängigen Partei (sog. Intermediär), der bei der Durchführung ihrer Aufgaben vertraut werden muss. Auch in technischen Bereichen finden sich Intermediäre, zum Beispiel bei Anbietern von Cloud-Plattformen oder sozialen Netzwerken, deren Verhalten für Konsumenten häufig nicht transparent ist. Nutzer von Diensten wie Facebook, Google+ oder Twitter können kaum nachvollziehen, welche Daten erhoben, wie diese verarbeitet und gespeichert werden. Die Blockchain kann die Nutzung privater Daten für den jeweiligen Nutzer besser kontrollierbar und transparenter machen. Ein auf der Blockchain basierendes Identitätsmanagement soll dabei Anwendung finden.



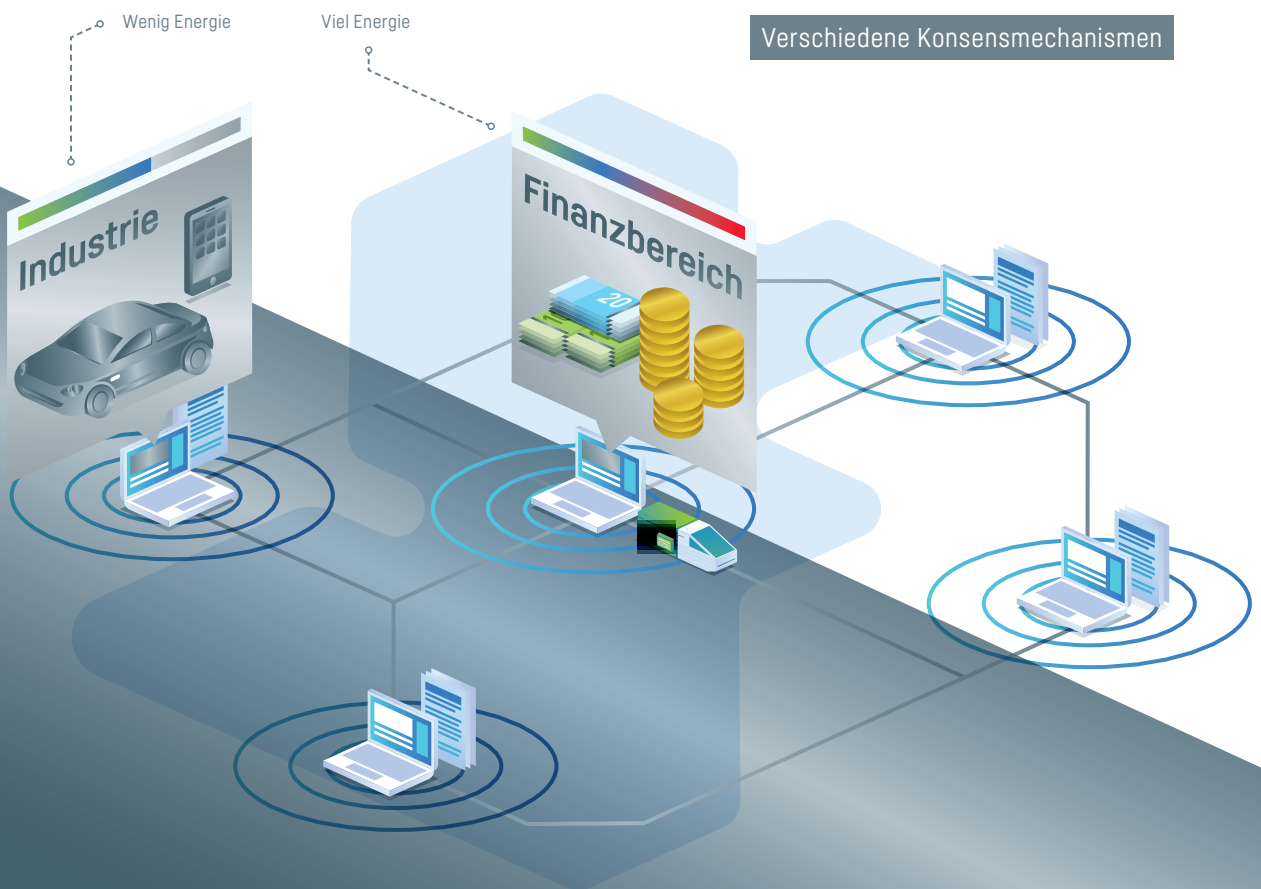
Datensicherheit: Fälschungssicherheit

Jede neue Transaktion wird an alle Computer eines Netzwerks (sog. Knoten, engl. nodes) weitergeleitet. Jeder dieser Knoten prüft die Transaktion auf Gültigkeit. Ein bis ins Jahr 2008 noch ungelöstes Problem bei dieser Prüfung war, das mehrfache Weiterleiten derselben Daten (dieses wird auch als Double-Spending-Problem bezeichnet) in einem voll dezentralen System unter Ausschluss eines Intermediäres (bspw. einer Bank) festzustellen. Das Double-Spending-Problem wurde auf rein algorithmischer Ebene ohne Notwendigkeit eines Intermediäres bei der Blockchain gelöst. Ein essenzieller Bestandteil dieser Lösung ist der sogenannte Konsensmechanismus, der die verschiedenen Knoten in der Blockchain synchronisiert und eine Art Abstimmung über die Aufnahme neuer Daten durchführt. Einer der möglichen und der derzeit am weitesten verbreitete Konsensmechanismus ist der „Proof of Work“. Dabei müssen die Knoten unter großem Einsatz von Energie und Rechenleistung ein Zufallswort generieren, das eine bestimmte Voraussetzung erfüllt. Der erste Knoten, dessen Zufallswort diese Voraussetzung erfüllt, wird für seine Mühen (also Energie und Rechenleistung) entlohnt.



Mit „Mining“ wird in der Blockchain-Technologie die Teilnahme an der Konsensfindung (Verhinderung von Double-Spending-Problemen) bezeichnet, wobei die Teilnahme an der Konsensfindung den Einsatz einer gewissen Ressource (Speicherplatz, Elektrizität o. Ä.) erfordert. Um Nutzer zu motivieren an der Konsensfindung teilzunehmen, wird als Gegenleistung für den Einsatz der Ressourcen ein meist geldwerter Anreiz (Incentive) geschaffen – häufig in Form von Coins.

Zwischenzeitlich gibt es weitere Mechanismen, die den Konsens erheblich effizienter erzeugen, also mit deutlich weniger Zeit- und Energieaufwand.





Datensicherheit: Zugriffsschutz

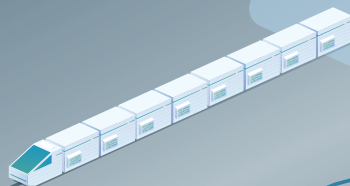
Ein zweiter Mechanismus, der die Nutzung der Blockchain absichert, ist die Ver- und Entschlüsselung von Daten. Um eine Transaktion zu tätigen, muss der jeweilige Nutzer zuerst bestätigen, dass er berechtigt ist, auf die Daten der Transaktion zuzugreifen. Dazu werden digitale Signaturen eingesetzt. Digitale Signaturen werden unter Verwendung eines privaten Schlüssels [Private Key] und eines zu signierenden Datensatzes [bspw. einer Transaktion] erstellt. Die digitale Signatur ist eindeutig und kann mithilfe des öffentlichen Schlüssels [Public Key] des Nutzers überprüft werden. Somit kann sichergestellt werden, dass eine digital signierte Transaktion tatsächlich von einem Nutzer vorgenommen wurde.

Über diese digitale Signatur kann eindeutig verifiziert werden, welcher Nutzer dazu berechtigt ist, einer Transaktion einen Nachfolger zuzuordnen, also Daten einer Transaktion weitergeben darf.

Zusammenfassung

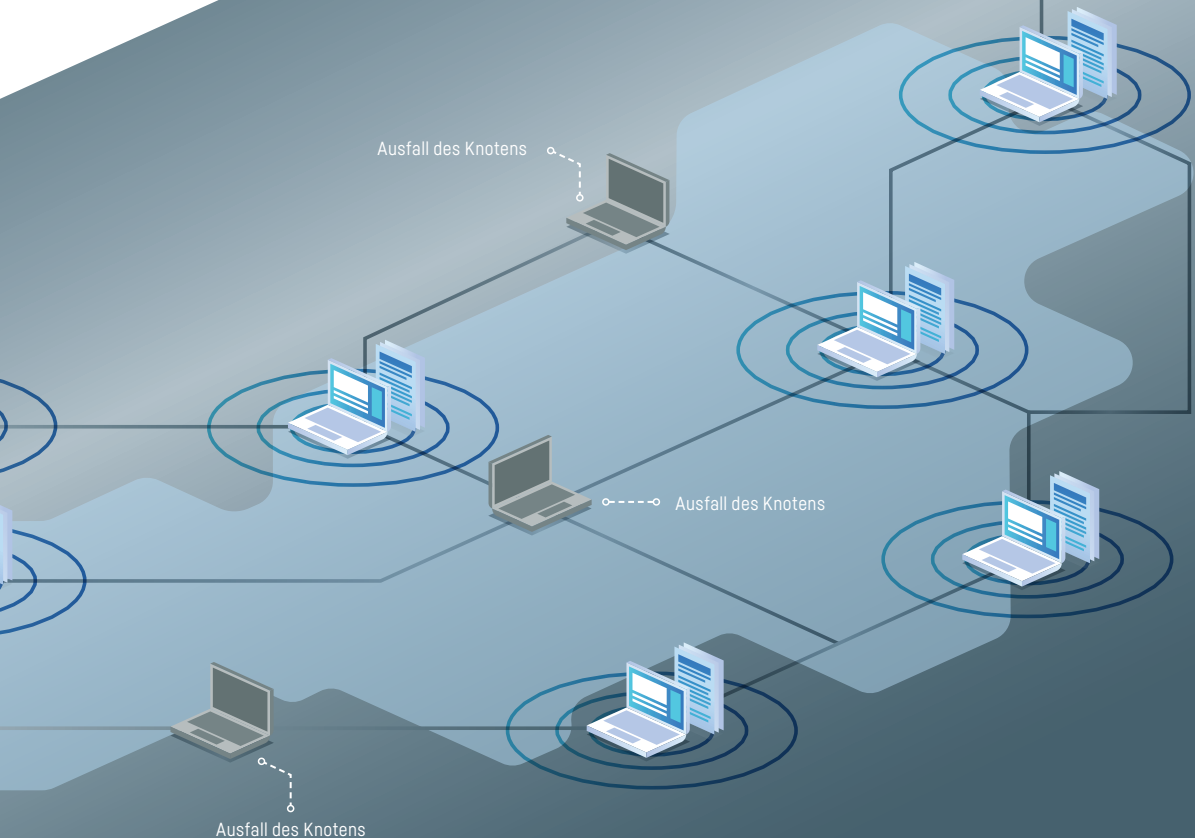
Der Einsatz der DLT ist vor allem dann sinnvoll, wenn mehrere Parteien, die sich gegenseitig nicht vertrauen, Daten miteinander teilen wollen; wenn von großem Interesse ist, dass diese Daten nicht zentral von einer Partei gehalten werden; und wenn deren Übertragung unveränderbar und nachvollziehbar sein soll. Die DLT schafft auf Datenbasis Transparenz zwischen sich nicht vertrauenden Parteien und kann Prozesse beschleunigen bzw. automatisieren. Darüber hinaus ist die DLT in hohem Maße verfügbar. Beim Ausfall einiger Knoten des verteilten Registers kann ein Dienst mit den verbliebenen weiterbetrieben werden. Transaktionen können unter Verwendung der DLT meist schneller und unter Umständen sogar kostengünstiger durchgeführt werden, als wenn sie über einen Intermediär abgewickelt würden. Durch die besonders hohe Integrität der DLT wird gewährleistet, dass Transaktionen unveränderbar gespeichert werden.

Mehrere Parteien, die sich nicht vertrauen



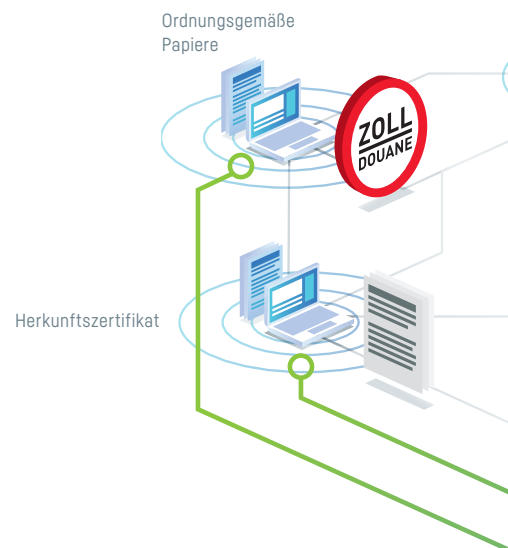
Qualität

- Hohe Verfügbarkeit
- Unveränderbarkeit der Datenspeicher
- Zusammenarbeit ohne Intermediär
- Verhindern betrügerischen Handelns einzelner Parteien auf Basis von Algorithmen



Mögliche Anwendungen

Die aktuellen Diskussionen konzentrieren sich auf die Nutzbarmachung der DLT zur Unterstützung von wirtschaftlichen und staatlichen Prozessen. Im größeren Rahmen könnte sogar die Übertragung von geistigem Eigentum auf einem verteilten Register festgehalten und in Echtzeit durchgeführt werden. Im „Supply Chain Management“ kann die DLT dazu genutzt werden, produktbezogene Daten zuverlässig und nicht manipulierbar zu speichern und Übergabeprotokolle zu digitalisieren. Bereits heute bietet eine solche, auf der DLT basierende Dokumentation die Möglichkeit zu prüfen, ob z. B. ein Rohstoff ein Konfliktmineral ist.



Blockchain

Just in time



Bezahlungsvorgänge
Einkauf/Verkauf



Faire
Lohnzahlung

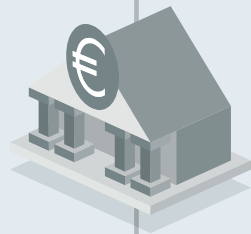
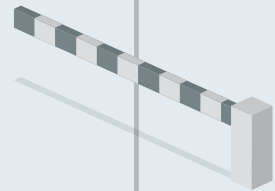
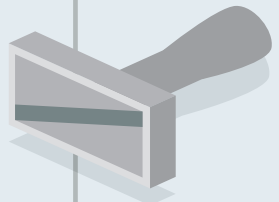


Zertifikat



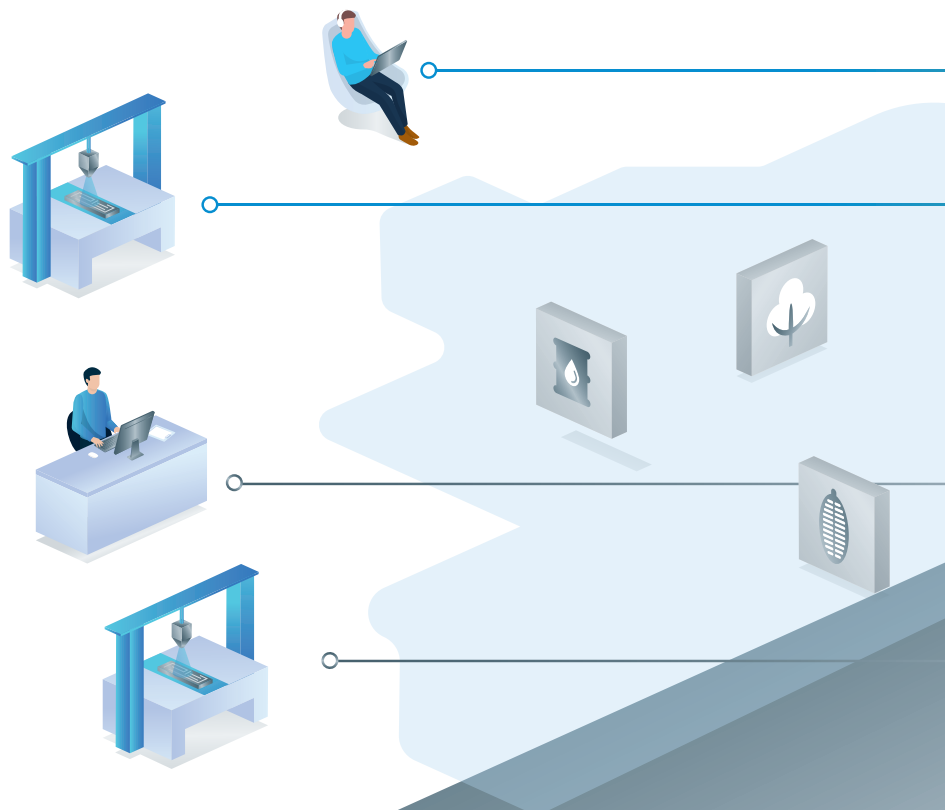
Herkömmlicher Weg

Zeitaufwand



BLOCKCHAIN

Für komplexere Anwendungen wird großes Potenzial in „Smart Contracts“ gesehen. Dabei handelt es sich um Programme, die maschinenlesbare formalisierte Regeln enthalten und auf einem verteilten Register mit einer festen Adresse gespeichert werden. Sie können sowohl auf Daten zugreifen, die auf dem verteilten Register gespeichert sind, als auch auf externe Dienste. Durch Smart Contracts ist es bspw. möglich, Zugriffsrechte für Dritte auf private Daten zu definieren, wie den Zugriff auf die eigene Krankenakte im Rahmen von medizinischen Untersuchungen. Auch die Kommunikation zwischen Maschinen im Internet der Dinge und die Zugriffsverwaltung auf die Maschinen selbst



kann durch die DLT und Smart Contracts sicherer und transparenter gestaltet werden. So könnten in Zukunft Elektroautos den zum Laden bezogenen Strom selbst und automatisch mit einer Kryptowährung bezahlen.

Es gibt bereits unzählige Anwendungsgebiete und Szenarien, in denen die DLT einen vielversprechenden Beitrag bzgl. der Sicherheit und Transparenz von genutzten Systemen liefert oder liefern kann. Dabei wird schon heute deutlich, dass die DLT in naher Zukunft eine erhebliche strukturelle Veränderung bisheriger Prozesse hervorrufen und dadurch unseren Alltag unterstützen wird.

